IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re:	David J. Wetherall	Confirmation No:	1582
Application No:	09/825,139	Group:	2153
Filed:	April 3, 2001	Examiner:	Barqadle, Yasin M.
For:	Independent Detection and Filtering of Undesirable Packets		
Customer No.:	29127		

Attorney Docket No.	0016.0007US1

APPELLANTS' REPLY BRIEF

Mail Stop Appeal Brief- Patents
Commissioner for Patents
P.O. Box 1450,
Alexandria, Virginia 22313-1450

Sir:

This is the Applicants' Reply to the Examiner's Answer mailed January 24, 2008 (Paper No.: Unnumbered).

Remarks

The arguments presented in pages 3 through the first half page 10 of the Examiner's Answer restate, *verbatim*, the positions set forth in the Final Office Action mailed February 6, 2007. It is believed that Applicants' position was adequately set forth in the Appeal Brief November 8, 2007 with respect to these arguments. Addressing these arguments, again, would not further clarify the issues for this appeal.

Somewhat new arguments were presented beginning at the second half of page 10 of the Examiner's Answer. These are addressed below:

Forwarding/Dropping Packets

Claim 1, for example, requires: handling the packet based at least in part on the result of said independent determination by...dropping the packet if the packet is deemed to be an undesirable packet."

Relative to this feature, the Examiner's Answer makes the following statement:

> The Appellant also argues that "to be sure, the Canion Application does not suggest dropping packets. See Canion application at paragraph [0185]. The packets are dropped depending upon whether they are deemed to be part of an attack." This argument seems to be a contradicting statement. As indicated above Canion teaches detecting incoming data packets in a network and determining whether to forward if it is authentic or drop the packet if it is undesirable packet (packets with potential security violations to protect the network against) (¶ 0177; ¶ 0183 and ¶ 0187). Therefore, the combined references of Primak and Canion teach the argued limitations.

The Appellants' Brief actually stated:

> The Canion Application also fails to show or suggest the feature of forwarding or dropping packets in dependence upon whether the packets are part of an existing conversation. To be sure, the Canion Application does suggest dropping packets. See Canion Application at paragraph [0185]. The packets are dropped depending upon whether they are deemed to be part of an attack. In contradistinction, the present claimed invention forwards or drops a packet depending on whether it is part of an existing conversation by reference to persistent information in the packet.

Appellants' Brief at page 8, emphasis added.

The misquote of the Appellants' Brief seems to characterize the Answer's misunderstanding of the claimed invention and the arguments for patentability. That is, the Appellant's are in fact conceding that the Canion Application teaches dropping of packets, but only in a general sense. In fact, Appellant's dispute that the Canion Application teaches to drop packets as claimed, *i.e.*, based on an "independent determination" that the packets are part of a conversation by reference to persistence information in the packets.

The Answer does not seem to assert that Canion Application discloses this specific, claimed mode or criteria for dropping packets. Thus, Appellant's maintain that these claimed distinctions advocate for the patentability of the independent claims.

Packet Dropping based on Age

Claim 9 requires "determining if time has elapsed more than a predetermined threshold since a time of first observation was recorded for the nonce, if the extracted nonce and the independently generated nonce are deemed to be the same and dropping the packet if the time has elapsed more than the predetermined threshold event though the extracted nonce and the independently generated nonce are deemed to be the same".

The Answer addresses this claim 9 and Appellants' arguments as follows:

> Examiner notes that the combined teaching of Primak in view Canion and further in view of Bull teach the argued limitation. Fore example Primak teaches the aging factor [col. 9, lines 20-67] while Canion teaches the taking action such as discarding packets when undesirable packet are detected through "the MAC header identification and verification, IP header identification and verification, IP header checksum validation, TCP and UDP header identification and validation, and TCP or UDP checksum validation. It also may perform the lookup to determine the TCP connection or UDP socket (protocol session identifier) to which a received packet belongs. Thus, the network interface engine verifies packet lengths, checksums, and validity." (¶ 065). Canion's system is flexible to take action such as discarding packets that are deemed undesirable in the network "It can take immediate action, such as discarding the packet or notifying the network administrator.... Thus, the security accelerator provides flexibility for providing counter measures to new security attacks as the new types of attacks become known." (¶ 0177 and ¶ 0183).

First, the Primak patent does not teach to monitor the age of packets or nonce contained in packets. Primak at col 9, lines 20-67 provides:

Each time a client **60** logs onto the web site, the plug-in **22** of the web server **20** sends the content ID of the client **60** to the dynamic content router **10**. The dynamic content router **10** compares the content ID of the client **60** against the entries in the content table **14**. If no matching content record is found in the content table **14** indicating that the client is a first time visitor of the web site, the dynamic content router **10** generates a new content record for the client **60** in the content table **14**. The new content record contains at least the content ID of the client **60**, the session server ID stored in the "last access server" field in FIG. **4**, and the login time and date of the client stored in the "last access time" field in FIG. **4**.

If the client **60** had previously logged onto the web site, then one of the content records in the content table **14** will contain the content ID of the client **60**. Accordingly, on each subsequent visit to the web site by the client **60**, the dynamic content router **10** locates the content record of the client **60** from the content table **14**. The content record of the client **60** includes the time and date of the client's last login or session and the identification of the application server **30** accessed by the client **60** in the last login (or the last accessed application server). If the client's current session server is same as the last accessed application server, the dynamic content router **10** updates the "last access time" field of the client's content record with the client's current session or login time and date.

However, if the client's current session server is different from the last accessed application server, the dynamic content router **10** determines whether the client's requests can be processed by the current session server or routed to another application server **30**. The dynamic content router **10** reads the database replication latency table **16** to compare the replication latency values of the database connected to the client's current session server and the database connected to the last accessed application server. If the replication latency of the two databases **42***a* and **42***b* (the period of time it takes to copy updated records from one database to the other) is less than the time elapsed between the client's last access time and the client's current login time (i.e., a session interval), the dynamic content router **10** determines that the current session server can process the client's requests and appropriately updates the last accessed application server field and the last access time field of the client's content record. That is, the last accessed application server field now identifies the current session server and the last access time now reflects the client's current login time and date. It is appreciated that if the client's current session

This section of Primak clearly describes the tracking of client login times and fails to bear any relevance to the claimed notion of using nonces as conversation identifiers and dropping packets based on observation times of nonces.

Moreover, the premise of the Answer seems to be that since one reference teaches an "aging factor" and another reference teach "discarding packets", albeit for completely different reasons, that it would be obvious to drop packets based on the time of first observation of a nonce, as claimed.

The arguments of the Answer undermine the touchstone of patentability: was the invention obvious to one skilled in the art at the time of the invention. The Answer, instead, substitutes a process of deconstructing the claims into a series of words and then finding those words in a prior art references. On the other hand, the Answer does not show why the claimed features would have been obvious or why one skilled the art would have picked a notion of one reference, monitor packet age, with a notion in another reference, drop packets.

In fact, the present claimed invention describes features and functionality that is not present in any of the applied reference: specific criteria for dropping packets. The failure of the references to provide even the separate features of the claim invention advocates for patentability. Litton Systems, Inc. v. Honeywell, Inc., 87 F.3d 1559 at 1569 (Fed. Cir. 1996).

Thus, withdrawal of the rejections is respectfully solicited.

For the foregoing reasons, Applicants believe that the pending rejections should be withdrawn, and that the present application should be passed to issue. Should any questions arise, please contact the undersigned.

Respectfully submitted,

Houston Eliseeva LLP

By /grant houston/
J. Grant Houston
Registration No.: 35,900
4 Militia Drive, Ste. 4
Lexington, MA 02421
Tel.: 781-863-9991
Fax: 781-863-9931

Date: March 24, 2008